EXHIBIT B

2019 WL 2211316
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

MICHAEL MCDONALD et al., Plaintiffs,
v.
KILOO APS et al., Defendants.
AMANDA RUSHING et al., Plaintiffs,
v.
THE WALT DISNEY COMPANY et al., Defendants.
AMANDA RUSHING et al., Plaintiffs,
v.
VIACOM INC. et al., Defendants.

Case No. 17-cv-04344-JD
|
Re: Dkt. No. 193, 195, 202, 204, 205 Case No. 17-cv-04419-JD
|
Case No. 17-cv-04492-JD
|
05/22/2019

JAMES DONATO, United States District Judge

ORDER RE MOTIONS TO DISMISS

***1** These cases are related actions brought by parents over gaming apps for kids. *McDonald v. Kiloo*, Case No. 17-4344, involves the "Subway Surfers" app. *Rushing v. The Walt Disney Company*, Case No. 17-4419, involves "Princess Palace Pets" and four versions of "Where's My Water?" *Rushing v. Viacom Inc.*, Case No. 17-4492, challenges "Llama Spit Spit." All of the cases are putative class actions and allege that the apps were used to track online behavior on a device and user-specific level, and that defendants exploited the data, without disclosure or consent, for profit. In effect, the complaints allege that the apps were covert collectors of behavioral data for delivery of targeted advertising to users, namely the kids who played the games.

Plaintiffs have sued a number of "developer defendants" and "SDK defendants." The developer defendants, which include Disney, Viacom, Kiloo and Sybo, are the companies that created the games and made them available for download. The SDK defendants are mobile advertising and app monetization companies that provide "software development kits" containing code to collect user data. These defendants include AdColony, Chartboost, Tapjoy, Flurry and other entities. Plaintiffs allege that the developer defendants embedded the SDK defendants' code into the games to gather and transmit to the SDK defendants "persistent identifiers" and personal data for tracking, profiling and ad targeting.

All the cases assert privacy claims under the California Constitution and for intrusion upon seclusion under California law. The *Disney* case adds a privacy claim under Massachusetts law.[1] The *Kiloo* and *Disney* cases also include consumer protection claims under New York's General Business Law § 349, and *Disney* further invokes the California Unfair Competition Law and the Massachusetts Unfair and Deceptive Trade Practices Statute.

The Court related the cases but did not consolidate them for trial. Plaintiffs filed amended complaints as a result of prior proceedings, mainly to avoid potential preemption under the federal Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 ("COPPA"). *See* Dkt. No. 159. Defendants seek to dismiss the amended complaints under Rule 12(b)(6) and in some cases for lack of personal jurisdiction, with several arguments made on a joint basis and others on a defendant-specific basis. This order resolves these motions.

BACKGROUND

The operative allegations are the same in all the cases, as tailored to the pertinent developers and SDK defendants for each game. The allegations in *Kiloo* are representative of the cases as a whole, and are used here as the context for the motions.

As alleged in the *Kiloo* amended complaint (Dkt. No. 268-1, "KAC"), a parent or child downloads and installs a gaming app onto a cell phone or other mobile device for play. KAC ¶ 28. When the app is launched, it connects immediately to a server hosted by the developer and begins sending data even before the user plays the game. *Id.* ¶ 40. The data sharing is invisible to the user. *Id.* As the user plays the game, the embedded SDK code communicates with the SDK defendant's individual server. *Id.* ¶ 42. The SDK code sends requests or "calls" for an ad to the server,

and the user's personal data is sent with each call. *Id.* As a result of the call, the user "may receive a single ad, but nonetheless multiple SDKs have exfiltrated to their servers the user's Personal Data." *Id.* The advertisements displayed in the gaming app to the user can be "video ads, wherein users 'watch a video ad and are rewarded with virtual currency.' " *Id.* ¶¶ 46, 99. The user might also be shown "pop-up ads between game plays." *Id.* ¶¶ 131-132. These ads "are targeted at specific users based on complex profiles assembled using their persistent identifiers, and other information bundled with those identifiers and sent to the SDK Defendants pursuant to the SDK coding inputted into the app and downloaded onto users' devices." *Id.* ¶ 133.

***2** The KAC alleges that the user data harvested by the SDKs includes (1) an ID for Advertisers ("IDFA") and ID for Vendors ("IDFV") for Apple devices; (2) an Android Advertising ID ("AAID") and Android ID for Android devices; (3) the device's International Mobile Equipment Identity ("IMEI"); (4) the specific device name; (5) IP address; (6) timestamp, *i.e.*, the time at which an advertising event is recorded; and (7) Device Fingerprint data, including the user's language, time zone and country, and mobile network or carrier. *See*, *e.g.*, KAC ¶¶ 47-52. Plaintiffs allege that the SDK defendants retain this user data. SDKs "store[ ] and analyze[ ] the Personal Data to enable continued tracking of the user, such as what ads she has already seen, what actions she took in response to those ads, other online behavior, and additional demographic data." *Id.* ¶ 42. This allows the SDK defendants -- "and other entities in the ad network" -- to "monitor, profile, track her over time, across devices, and across the Internet." *Id.*

Plaintiffs supplement these allegations with facts specific to several of the SDK defendants. Flurry is said to assign a unique ID number to each user to continue tracking them within the Flurry database. *Id.* ¶ 64 n.33. It combines personal information directly gathered on users "with information received about users from third-parties" such as Facebook or Twitter, as well as "user activity on other sites and apps." *Id.* ¶ 65. Flurry "shares information it collects from its users within its affiliated brands and with 'publishers, advertisers, measurement analytics, apps, or other companies." *Id.* ¶ 66. The information collected on a user includes "name, gender, birthdate, geolocation information, search queries, mobile device identifier, mobile phone number, alternative email addresses, contacts, contact information (including online contact information), nicknames and aliases, physical address, IP address, other persistent identifiers, and any other information [a] child [user] may share with [Flurry] or [Flurry's] partners, such as photos, videos or audio files that contain [a child user's] image or voice." *Id.* ¶ 67.

SDK Vungle is alleged to have the capacity to "share Personal Data with other, undisclosed third-parties," and plaintiffs allege that their forensic analysis shows that Vungle sent a user's IDFA/AAID and other personal data to a "separate online marketing company called Adjust." *Id.* ¶ 73. This transmission "permitted Adjust to track the user's activities subsequent to viewing the ad." *Id.* Such tracking, "known as 'ad attribution,' " enables online marketing companies to "track users on behalf of advertisers, observing the users' behavior over time to determine whether an ad leads a user to install the advertised app and, thus, whether a specific ad influenced behavior and was commercially profitable." *Id.* SDK defendants AdColony and Flurry are alleged to have advertised their ability to accomplish ad attribution "even where users have attempted to limit ad tracking." *Id.* ¶¶ 137(a), (b). Similar allegations are made about the other SDK defendants. SDK Kochava is alleged to have marketed its ability to "match individual users to their devices using what it calls 'cross-device algorithms.' " Dkt. No. 117-1 ("DAC") ¶ 58. These algorithms purportedly allowed Kochava to "track user behavior and to identify users -- including children -- at the individual level, even where there are multiple users of the same device." *Id.*

The gravamen of the complaints is that the "Developer Defendants and the SDK Defendants, in coordination, collect and use the Personal Data described [in the complaint] to track, profile, and target children with targeted advertising." KAC ¶ 110. Plaintiffs allege that "[w]hen children are tracked over time and across the Internet, various activities are linked to a unique and persistent identifier to construct a profile of the user of a given mobile device." *Id.* ¶ 111. While a persistent identifier in isolation is a "string of numbers uniquely identifying a user," when "linked to other data points about the same user, such as app usage, geographic location (including likely domicile), and Internet navigation, it discloses a personal profile that can be exploited in a commercial context." *Id.* Plaintiffs allege that defendants "aggregate this data, and also buy it from and sell it to other third-parties." *Id.* ¶ 112. Plaintiffs add

that personal digital devices "are increasingly associated with individual users, rather than families," and that even children often "have their own devices; as of 2017, 45% of children younger than 8-years-old had their own mobile device." *Id.* ¶¶ 117, 144.

***3** Plaintiffs contend that "[t]he ability to serve targeted advertisements to (or to otherwise profile) a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (name, email addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used in conjunction with other data points to build robust online profiles." *Id.* ¶ 122. "Once a persistent identifier is sent 'into the marketplace,' it is exposed to -- and thereafter may be collected and used by -- an almost innumerable set of third-parties." *Id.*

LEGAL STANDARDS

The standards governing defendants' motions to dismiss are well-established. Rule 8(a)(2) of the Federal Rules of Civil Procedure requires that a complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." To meet that rule and survive a Rule 12(b)(6) motion to dismiss, a plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This does not impose a probability requirement at the pleading stage. "[I]t simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of" the conduct challenged by plaintiff. *Id.* at 556. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). The allegations in the complaint must be sufficiently clear and concrete to give the defendant an "idea [of] where to begin" in preparing a response to the complaint. *Twombly*, 550 U.S. at 565 n.10. Determining whether a complaint states a plausible claim for relief is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 679.

The Court treats the plaintiffs' factual allegations as true and draws all reasonable inferences in plaintiffs' favor. *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). But it will not "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quotation omitted). If the complaint is dismissed, an opportunity to amend will be provided unless the Court determines that no cure is possible by new allegations of fact. *Lopez v. Smith*, 203 F.3d 1122, 1130-31 (9th Cir. 2000).

For the motions to dismiss for lack of personal jurisdiction, plaintiffs bear "the burden of establishing that jurisdiction is proper." *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008). Where, as here, the Court has not required an evidentiary hearing, it is enough for the plaintiff to make a prima facie showing of personal jurisdiction. *Id.* Uncontroverted allegations in the complaint must be taken as true, and "[c]onflicts between the parties over statements contained in affidavits must be resolved in the plaintiff's favor." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004). However, the Court "may not assume the truth of allegations in a pleading which are contradicted by affidavit." *Mavrix Photo, Inc. v. Brand Technologies, Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011). There are two types of personal jurisdiction, "general" and "specific," and for the Court to exercise the latter over a defendant, "the suit must arise out of or relate to the defendant's contacts with the forum." *Bristol-Myers Squibb Co. v. Superior Court of California, San Francisco County*, 137 S.Ct. 1773, 1779-80 (2017) (quotations omitted).

DISCUSSION

I. STATE LAW PRIVACY CLAIMS

A. California Intrusion Upon Seclusion

***4** A California tort claim for intrusion upon seclusion is alleged for all named plaintiffs and putative class members. While plaintiffs pursue the tort on behalf of a proposed 34-state class in all three cases, the named plaintiffs themselves are from California (*Kiloo*, *Disney* and *Viacom* cases), New York (*Kiloo* and *Disney* cases) and Massachusetts (*Disney* case only). [2]

For the elements of the tort, plaintiffs say that (1) they and their children had "reasonable expectations of privacy in their mobile devices and their online behavior"; (2) defendants "intentionally intruded on and

into plaintiffs' and class members' solitude, seclusion, or private affairs by intentionally designing" the games and SDKs to "surreptitiously obtain, improperly gain knowledge of, review, and/or retain plaintiffs' and class members' activities through the monitoring technologies and activities" described in the complaints; and (3) these intrusions were "highly offensive to a reasonable person." KAC ¶¶ 227-231; DAC ¶¶ 249-253; Dkt. No. 90-1 ("VAC") ¶¶ 169-173. Plaintiffs contend that "California law on intrusion upon seclusion is applicable for all members of the Intrusion Upon Seclusion Class because there is no conflict of law between the law in California and any of the states in which the Class members reside. The jurisprudence in California and each of the relevant states adheres to Restatement (Second) of Torts, § 652B with no material variation." KAC ¶ 225; DAC ¶ 247; VAC ¶ 167. Defendants do not disagree on the choice-of-law issue and focus on California law for their joint arguments to dismiss this claim. *See* Dkt. No. 193.

The Court is sitting in diversity jurisdiction and is guided principally by decisions of the California Supreme Court. Three cases in particular are key to plaintiffs' privacy claims. In *Hill v. National Collegiate Athletic Association*, 7 Cal. 4th 1 (1994), the California Supreme Court discussed state privacy law in the context of a claim under the "Privacy Initiative," a voter initiative which added the phrase "and privacy" to the California Constitution, article I, section 1 in November 1972. As amended, the section states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

Examining a claim brought by student athletes who were required to provide urine samples under closely monitored conditions, the *Hill* court held that "a plaintiff alleging an invasion of privacy in violation of the state constitutional right to privacy must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." 7 Cal. 4th at 39-40. For the last element, the court stated that "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Id.* at 37. The court also observed, more than once, that "privacy interests and accompanying legal standards are best viewed flexibly and in context," and "[w]hatever their common denominator, privacy interests are best assessed separately and in context." *Id.* at 31, 35. The court ultimately concluded there was no constitutional privacy violation and reversed the permanent injunction against the NCAA's drug testing program, both because student athletes had diminished expectations of privacy in that context and the NCAA had competing interests that were "reasonably calculated to further its legitimate interest in maintaining the integrity of intercollegiate athletic competition." *Id.* at 44. On the seriousness of the privacy invasion, the court held that the "NCAA's use of a particularly intrusive monitored urination procedure justifies further inquiry, even under conditions of decreased expectations of privacy." *Id.* at 43.

***5** Four years later, in *Shulman v. Group W Productions, Inc.*, 18 Cal. 4th 200 (1998), the court examined two privacy claims brought under the common law rather than the state Constitution. Citing the Restatement Second of Torts sections 652A-652E, the court differentiated the claim alleging "public disclosure of private facts" from the claim alleging "intrusion into private places, conversations, or other matters." *Id.* at 214. Both were described as privacy causes of action recognized by California courts. Characterizing the latter as the privacy tort that "best captures the common understanding of an 'invasion of privacy,' " the court explained that the claim has two elements: "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Id.* at 230-31. Determining the offensiveness of an intrusion "requires consideration of all the circumstances of the intrusion, including its degree and setting and the intruder's 'motives and objectives.' " *Id.* at 236 (quotation omitted). The *Shulman* court echoed *Hill* in stating that "California tort law provides no bright line on this question; each case must be taken on its facts." *Id.* at 237. On the intrusion claim in that case, the court held that summary judgment for the defense was improper because there were triable issues of fact on both plaintiffs' expectations of privacy and the offensiveness of the intrusion. *Id.* at 230-43.

In *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272 (2009), the court considered invasion of privacy claims under the common law and the state Constitution. This case involved a hidden camera set up in plaintiffs' shared office in an attempt by their work supervisor to determine who

might be making improper use of the work computer in that office. In analyzing plaintiffs' claims, the court looked to *Shulman* for the elements of the common law tort claim, and to *Hill* for the elements for the constitutional claim. 47 Cal. 4th at 286-87. Significantly, the *Hernandez* court "[b]orrow[ed] certain shorthand language from *Hill*, 7 Cal. 4th 1, 26, which distilled the largely parallel elements of these two causes of action," and analyzed the two claims together, considering "(1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." 47 Cal. 4th at 288. On the question of whether "defendants' video surveillance measures intruded upon plaintiffs' reasonable expectations of privacy," the court agreed with the Court of Appeal that plaintiffs had plausibly made out a prima facie case in the affirmative. *Id.*

For the inquiry into the "offensiveness/seriousness of the privacy intrusion," the court observed that actionable invasions of privacy "must be 'highly offensive' to a reasonable person (*Shulman*, 18 Cal. 4th at 231), and 'sufficiently serious' and unwarranted as to constitute an 'egregious breach of the social norms.' (*Hill*, 7 Cal. 4th at 37)." *Id.* at 295. The court held that "no reasonable jury could find in plaintiffs' favor and impose liability on this evidentiary record," where "[a]ctivation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns" and plaintiffs "were not at risk of being monitored or recorded during regular work hours and were never actually caught on camera or videotape." *Id.* at 295, 301.

As these cases indicate, the California Supreme Court has moved toward treating the tort and constitutional privacy inquiries as functionally identical, although the claims do continue to exist as separate claims with technically distinct elements. Consequently, plaintiffs were right to allege for the standalone intrusion claim that the intrusions were "highly offensive to a reasonable person." KAC ¶ 230; DAC ¶ 252; VAC ¶ 172. By the same token, defendants were wrong in trying to marginalize as "irrelevant" certain consumer surveys proffered by plaintiffs for the tort claim because they did not ask about an "egregious breach of social norms." Dkt. No. 193 at 10.

Defendants' insistence on a sky-high standard of egregiousness is also questionable. Defendants say that "[o]nly the most egregious circumstances meet this standard, such as dissemination by the police of gruesome photographs of a deceased car accident victim, disclosure of a patient's HIV status, or misrepresenting one's identity to access confidential information about childhood abuse." *Id.* at 5. There is no doubt those would be egregious acts, but neither the law nor common sense demand that "egregious" be cabined to such extraordinary circumstances and nothing more.

***6** The cases defendants cite certainly do not point to a different conclusion. In *Catsouras v. Department of California Highway Patrol*, 181 Cal. App. 4th 856 (2010), which involved a callous circulation of gruesome death images, the claim at issue was based on the public disclosure of private facts and not an intrusion upon seclusion, and so the court did not apply *Hill*'s "egregious breach of social norms" standard at all. The *Catsouras* case in fact makes no mention of *Hill*, and specifically notes that another case is "inapposite" precisely because it discussed "a claim of invasion of privacy in the guise of intrusion into seclusion, not public disclosure of private facts." 181 Cal. App. 4th at 869. *Urbaniak v. Newton*, 226 Cal. App. 3d 1128 (1991), which addressed the disclosure of a patient's HIV status, is a decision from a California intermediate appellate court that pre-dates *Hill*. And *Taus v. Loftus*, 40 Cal. 4th 683, 730-739 (2007), focused its analysis of plaintiff's intrusion claim on the reasonableness of her expectation of privacy. While the *Taus* court found that the conduct alleged in that case -- misrepresenting one's identity to access confidential information about plaintiff's childhood abuse -- "could be found 'highly offensive' for purposes of the intrusion-into-private-matters tort," *id.* at 740, its factual context bears scant relevance here, and so the opinion is properly given little weight under the *Shulman* court's teaching that for offensiveness, "each case must be taken on its [own] facts." 18 Cal. 4th at 237; *see also Hernandez*, 47 Cal. 4th at 237.

Defendants also overstate the propriety of terminating privacy claims at the motion to dismiss stage. To be sure, the plausibility of a privacy claim may be decided on the adequacy of the offensiveness element as a matter of law. *See Deteresa v. American Broadcasting Cos., Inc.*, 121 F.3d 460, 465 (9th Cir. 1997) ("If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law.") (quoting *Sanders v. American Broadcasting Cos.*, 52 Cal. App. 4th 543 (1997)). But the Court is mindful of the

emphasis in *Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992 (2009), which involved a constitutional privacy claim, on the importance of having an adequate factual record before dismissing a privacy case. There, plaintiffs "allege[d] that the 49ers' patdown policy violate[d] their state constitutional right to privacy." *Id.* at 998. The court noted that the "case comes before us after the superior court dismissed the case on demurrer. This means that the 49ers' have not yet even filed an answer, given any explanation or justification for the alleged search policy, or asserted any defenses. The only record we have, and all we have to go by in deciding this case, is the complaint." *Id.* The *Sheehan* court concluded that, "given the absence of an adequate factual record,...further inquiry is necessary to determine whether the challenged policy is reasonable." *Id.* at 1003; *see also Hill*, 7 Cal. 4th at 40 ("[W]hether defendant's conduct constitutes a serious invasion of privacy [is] a mixed question[ ] of law and fact").

With this guidance in mind, the Court finds that plaintiffs have adequately alleged an intrusion upon seclusion claim and the offensiveness element in particular, which is the only element of the intrusion claim that defendants squarely challenge. *See* Dkt. No. 193. Plaintiffs state in detail what data was secretly collected, how the collection was done, and how the harvested data was used. They also present detailed and specific allegations about why these intrusions would have been highly offensive to the reasonable person on the basis of multiple sources, including reports, studies, surveys, case law and secondary legal materials. *See*, *e.g.*, KAC ¶¶ 149-166, *and cf. Hill*, 7 Cal. 4th at 36 ("Whether established social norms safeguard a particular type of information or protect a specific personal decision from public or private intervention is to be determined from the usual sources of positive law governing the right to privacy -- common law development, constitutional development, statutory enactment, and the ballot arguments accompanying the Privacy Initiative.").

***7** The observations by the California Supreme Court about the context-specific nature of the privacy inquiry, and that social norms on privacy are not static, are particularly apt here. *See, e.g., Shulman*, 18 Cal. 4th at 207-08; *see also Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1079-80 (N.D. Cal. 2016). Current privacy expectations are developing, to say the least, with respect to a key issue raised in these cases -- whether the data subject owns and controls his or her personal information, and whether a commercial entity that secretly harvests it commits a highly offensive or egregious act. The Court cannot say that the answers are so patently obvious that plaintiffs' allegations are implausible or inadequate as a matter of law.

Defendants again have not identified any cases that demand a different result. For example, in *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), the California Court of Appeal affirmed the dismissal of a constitutional privacy claim because "the supposed invasion of privacy essentially consisted of Lamps Plus obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements." The court found that "[t]his conduct is not an egregious breach of social norms, but routine commercial behavior." *Id.* The *Folgelstrom* court similarly affirmed the dismissal of the intrusion tort claim because, "[a]s with the alleged constitutional violation,...the conduct of which [plaintiff] complains does not meet the standard of 'highly offensive.' " *Id.* at 993.

The same does not hold here. Plaintiffs in this case have alleged that defendants harvested much more information about users than just their mailing addresses. They have also alleged that defendants are doing much more with the collected information than simply sending "coupons and other advertisements." Plaintiffs have alleged that defendants surreptitiously gathered user-specific information; they continue to gather information and track individual users in real time; they share (and buy and sell) this information with other third-party companies; and all of this results in the minor users being shown targeted advertisements and in the users continuing to be tracked after being shown the advertisements to see if they take actions in response to the ads. "[E]ach case must be taken on its facts" on the question of offensiveness, *Shulman*, 18 Cal. 4th at 237, and these sets of facts are not the same. This is not a case in which "the undisputed material facts show...an insubstantial impact on privacy interests." *Hill*, 7 Cal. 4th at 40. Plaintiffs have sufficiently pled more, and they are entitled to the development of an "adequate factual record" to more properly test their claims. *Sheehan*, 45 Cal. 4th at 1003.

In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016), also does not carry the day for defendants. The court addressed an intrusion upon

seclusion claim under New Jersey law, which, like California law, looks to the Second Restatements of Torts. 827 F.3d at 292. This Court agrees with *Nickelodeon* that the status of game users as minors is not a main driver of the privacy analysis, *see id.* 294-95, but the case is otherwise not germane. *Nickelodeon* affirmed the dismissal of Google because "courts have long understood that tracking cookies can serve legitimate commercial purposes." *Id.* at 294 & n.203 (citing, for example, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001)). Even if that debatable principle were embraced, it does not necessarily fit the scope of behavioral tracking that the mobile applications here are alleged to have practiced. As the United States Supreme Court has observed on several occasions, a mobile phone has become "almost a 'feature of human anatomy' " that provides a wealth of personal information about its user. *Carpenter v. United States*, 138 S.Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). Cell phones and mobile devices are "compulsively" carried and used by most people, *see*, *e.g.*, *Carpenter*, 138 S. Ct. at 2218, including kids. The persistent identifiers and other data harvested to track users on these ubiquitous mobile devices involve collection practices that exceed those of the cookies in *Nickelodeon*, and without a "long" understanding suggesting that that is okay to do.

***8** Defendants seek to downplay plaintiffs' complaints as alleging only the "collection of anonymous digital user data" and as lacking non-conclusory allegations of subsequent misuse. Dkt. No. 193 at 6. That is not a fair characterization of these detailed and lengthy complaints. When read in a common-sense way, as Rule 8 requires, plaintiffs' allegations are considerably more user-specific than defendants suggest and more than adequately allege that the collected data was used to serve plaintiffs with targeted advertising while using the apps.

This is enough to let the complaints go forward. The parties devoted considerable attention to a few other issues that do not need to be addressed at this stage of the case. One is deceit. The presence of an affirmative misrepresentation has been found significant by other courts. *See*, *e.g.*, *Nickelodeon*, 827 F.3d at 295, 269 (vacating dismissal of intrusion claim against Viacom where the registration form on Viacom's website included the message, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!," but plaintiffs alleged Viacom had nevertheless collected information and shared it with Google). While courts have found this kind of "plus" factor to be significant in establishing an expectation of privacy or making a privacy intrusion especially offensive, no court has held deceit to be a requirement of an intrusion claim. The parties do not suggest otherwise, and for the reasons discussed above, the Court concludes that plaintiffs here have sufficiently stated a claim even without that factor. The Court also notes that defendants have not challenged plaintiffs' expectation of privacy in any event, but only the gravity of the alleged invasion.

Both sides also discuss the contracts that existed between the developer defendants and the SDK defendants, as well as the defendants' respective privacy policies. [3] These documents will likely be pertinent to issues of notice and consent, and the ultimate resolution of plaintiffs' intrusion claims. As framed, however, they are not appropriate for resolution as a part of this 12(b)(6) analysis of whether or not plaintiffs have sufficiently stated an intrusion claim to go forward. *See*, *e.g.*, *Hill*, 7 Cal. 4th at 40 (defendant may prevail in a state constitutional privacy case by "pleading and proving, as an affirmative defense, that the invasion of privacy is justified because it substantively furthers one or more countervailing interests" or by pleading and proving "other available defenses, e.g., consent"); *Sheehan*, 45 Cal. 4th at 998 ("The Court of Appeal held that plaintiffs validly consented to the search policy. It may ultimately be right, but the meager record before us does not establish valid consent as a matter of law. In particular, the 49ers' have not demonstrated that the allegations of the complaint fail to state a cause of action under any possible legal theory. Further factual development is necessary."). Here, too, defendants have failed to demonstrate that plaintiffs' allegations fail to state a cause of action as a matter of law, and the issues of whether defendants complied with their contracts as written, Dkt. No. 193 at 18-19, and whether their privacy policies establish valid consent, *id.* at 19-20, are disputed issues that need further factual development.

B. California Constitution

***9** A claim for violation of privacy under the California Constitution is alleged for the California subclasses only. As discussed above, if this claim had been asserted in isolation, the elements would be: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy

in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill*, 7 Cal. 4th at 39-40. And in order to be actionable, the privacy invasion would need to "constitute an egregious breach of the social norms underlying the privacy right." *Id.* at 37.

The claim is not asserted here by itself but in combination with the tort claim of intrusion upon seclusion, which is alleged on behalf of all plaintiffs and putative class members. In that circumstance, it is appropriate to assess the two claims together and examine "the largely parallel elements" of these two claims which call on the Court to consider "(1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." *Hernandez*, 47 Cal. 4th at 288.

As discussed, the tort inquiry and constitutional inquiry are functionally identical. Defendants do not raise a separate challenge to the constitutional claim and no case points to a different outcome for this claim as opposed to the intrusion claim. Defendants' motion to dismiss the California constitutional claim is denied for the same reasons as for the California intrusion claim above.

C. Massachusetts Statutory Right to Privacy

A claim for a violation of Massachusetts' statutory right to privacy is asserted in the *Disney* case only. Massachusetts General Laws Chapter 214, § 1B guarantees freedom from "unreasonable, substantial or serious interference" with individual privacy.

Both sides agree that the analysis under this Massachusetts statute follows along the same lines as the California privacy claims. *See* Dkt. No. 193 at 14 (defendants); Dkt. No. 216-3 at 18 (plaintiffs). The Court concurs. *See Kelley v. CVS Pharmacy, Inc.*, No. 98-0897-BLS2, 2007 WL 2781163, at *2 (Mass. Super. Aug. 24, 2007) (statutory tort of invasion of privacy is established if plaintiff can show that "the interference was unreasonable and either substantial or serious"). Defendants' motion to dismiss the Massachusetts statutory right to privacy claim is consequently denied for the same reasons as the privacy claims under California law.

II. STATE LAW CONSUMER PROTECTION CLAIMS

A. New York GBL § 349

A claim under New York's consumer protection statute, New York General Business Law § 349(a), is asserted in the *Kiloo* and *Disney* actions. That statutory section prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [New York]."

Defendants argue that the types of privacy invasions alleged here are not actionable under GBL § 349, pointing to *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592 (NRB), 2016 WL 5080131 (S.D.N.Y. Aug. 17, 2016), *aff'd*, 684 Fed. Appx. 32 (2d Cir. 2017). There, the Southern District of New York court held that the statutory requirement of "actual" harm had not been met, and that plaintiffs had "not alleged a privacy harm actionable under GBL § 349" where they conceded "there are no allegations that PulsePoint was able to link [internet browsing history] information to specific persons, rather than to a particular browser and/or device." 2016 WL 5080131, at *11. Here, however, plaintiffs' complaints contain non-conclusory allegations that defendants collected and used personal data that is "identifiable or associable with specific, individual child users, is as persistent as a social security number, and can be used to track, profile, and target children across multiple devices and over time." KAC ¶ 254; *see also, e.g.*, DAC ¶ 58. And as discussed above, plaintiffs here allege much broader and deeper tracking than the mere collection of web browsing history. *See Mount*, 2016 WL 5080131, at *2 ("[B]esides its conclusory reference to users' 'Personally Identifiable Information,' the amended complaint does not specify what information other than web browsing history PulsePoint was able to acquire or how PulsePoint was able to acquire it."). The New York GBL § 349 claim will go forward.

B. California UCL

***10** A claim under the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, is asserted in the *Disney* case only. Of the two California plaintiffs in that case, Rushing and Remold, it is alleged for Remold only, presumably because she was the only one who paid any money to download one of the gaming apps at issue ("Where's My Water?"). Remold asserts a UCL claim under all three prongs of the UCL -- "fraudulent," "unfair" and "unlawful." DAC ¶¶ 281-284.

The Court denies defendants' motion to dismiss Remold's claim under the "unlawful" prong. As detailed above, the Court finds plaintiffs' California privacy claims can go forward, and so the UCL "unlawful" claim can also go forward on that basis.

Remold's "unfair" claim can also go forward. As our circuit noted in *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 866 (9th Cir. 2018), "the proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." In that case, the parties had argued unfairness under the competing tests in both *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Company*, 20 Cal. 4th 163 (1999), and *South Bay Chevrolet v. General Motors Acceptance Corporation*, 72 Cal. App. 4th 861 (1999). *Id.* at 866. *Hodsdon* expressly observed that "[t]he *Cel-Tech* test did not apply to actions by consumers," even though some California courts have extended the *Cel-Tech* definition of unfairness to consumer actions anyway. *Id.* The court rejected plaintiffs' claims under the *Cel-Tech* test but also examined the claims under the *South Bay* test, which dictates that "unfair" conduct occurs when the alleged practice "offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Id.* In light of the Court's rulings on the sufficiency of plaintiffs' pleadings for privacy invasions, including under the California Constitution, the Court cannot rule out at this stage that plaintiffs may also be able to prevail on a claim for an "unfair" violation of the UCL.

Finally, plaintiffs also assert a fraudulent omission claim under the UCL. DAC ¶ 281. That claim is subject to the heightened pleading standard under Federal Rule of Civil Procedure 9(b). The Court finds that plaintiffs' allegations clear that bar. Plaintiffs' allegations are "sufficient[ly] detail[ed]...to give us some assurance that [plaintiff's] theory has a basis in fact." *Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 989-90 (9th Cir. 2008). They also provide defendants "notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Bly-Magee v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001) (quotation omitted). Rule 9(b) "requires no more." *Berson*, 527 F.3d at 990.

C. Massachusetts GL 93A

A claim under Massachusetts' consumer protection statute, General Laws Chapter 93A, is asserted in the *Disney* case only. Plaintiff Supernault is the sole Massachusetts resident in that case. DAC ¶ 4.

Plaintiff contends that she has sufficiently pled an injury under that statute because she has pled "that she purchased the app (DAC ¶ 285)." Dkt. No. 213 at 2. But as defendants rightly point out, the cited paragraph relates to plaintiff Remold, not plaintiff Supernault. *See* DAC ¶ 285 ("Plaintiff Remold suffered injury in fact and lost money or property as a result of the defendants' business acts and/or practices. But for defendants' unfair, unlawful, or fraudulent business acts or practices, plaintiff Remold would not have purchased defendants' Where's My Water? app."). Plaintiff Supernault is alleged only to have downloaded the "Where's My Water? Free" and "Where's my Water? 2" apps, both of which appear to have been offered for free. DAC ¶¶ 4, 27.

***11** Because plaintiffs' argument that plaintiff Supernault suffered "injury or harm worth more than a penny," Dkt. No. 213 at 2 (citing *O'Hara v. Diageo-Guinness, USA, Inc.*, 306 F. Supp. 3d 441, 453 n.1 (D. Mass. 2018)), is not supported by their allegations, defendants' motion to dismiss this claim is granted. Plaintiffs will be given an opportunity to amend.

III. THE FLURRY AND OATH DEFENDANTS' MOTION TO DISMISS (DKT. NO. 204)

The Flurry and Oath defendants (Flurry, Inc., Oath (Americas) Inc. and Oath Inc.) separately move in the *Kiloo* action for a dismissal on the basis that plaintiffs' allegations "fail to differentiate among the three different entities, and fail to allege facts that could support liability of the Oath Entities for the acts of their subsidiary." Dkt. No. 204 at 2. Plaintiffs clarify in response that they are not alleging any theories of secondary liability. Dkt. No. 211 at 4.

Defendants' first point has merit. The complaint simply defines "Flurry" to include all three entities. *See* KAC ¶ 13 ("Flurry, Inc., Oath (Americas) Inc., and Oath Inc., together, 'Flurry' "). No factual basis is alleged for disregarding these entities' separate corporate forms in this manner. The complaint fails to give these defendants adequate notice of the claims against each of them, and their motion to dismiss is consequently granted. *See In re Resistors Antitrust Litigation*, No. 15-cv-03820-

JD, 2017 WL 3895706, at *4 (N.D. Cal. Sept. 5, 2017) (The "indiscriminate and generalized lumping together of defendants does not make for a sound pleading approach"). Plaintiffs will have an opportunity to amend.

IV. DEFENDANT SYBO'S MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM AND LACK OF PERSONAL JURISDICTION (DKT. NO. 205)

A. Failure to State a Claim - Sufficiency of Allegations Against Sybo

Defendant Sybo moves to dismiss the *Kiloo* complaint because, it argues, the complaint does not allege that "Sybo actually engaged in invasive or deceptive conduct," and instead alleges only that Sybo had a contractual relationship with Kiloo. Dkt. No. 205 at 1. This is not a fair characterization of the complaint's allegations against Sybo.

The complaint sufficiently alleges Sybo's involvement for 12(b)(6) purposes. *See*, *e.g.*, KAC ¶ 6 (Sybo "co-developed Subway Surfers"); ¶ 8 ("in addition to developing and marketing Subway Surfers, Sybo owns the intellectual property rights for Subway Surfers, and is responsible for developing the game play, graphics, and in-game programming"); n.2 (Sybo's "website contains animated graphics of Subway Surfers" and "links to another page identifying the vendors where consumers can download the game"); ¶ 9 ("Kiloo and Sybo equally split between them all revenues derived from Subway Surfers, including all revenue derived from advertising."). This is enough at this stage.

B. Lack of Personal Jurisdiction for New York Plaintiffs' Claims

Sybo additionally argues that the claims asserted by named plaintiff Tamara Draut (a New York resident) and other unnamed class members who do not live in California should be dismissed for lack of personal jurisdiction, because the connection to California is insufficient for those claims to bestow jurisdiction over Sybo for them in a California court. Dkt. No. 205 at 2 (arguing that plaintiffs "do not allege any facts about Sybo in support of their theory that New York residents can assert claims in a California court against a wholly Denmark-based defendant for alleged injuries that were presumably sustained in New York.").

***12** Plaintiffs argue only for the exercise of specific jurisdiction over Sybo; they make no arguments about general jurisdiction. Dkt. No. 210-4 at 7-9. As for the right standard for determining the existence of specific jurisdiction over Sybo, the Court declines plaintiffs' argument that *Bristol-Myers Squibb*, 137 S.Ct. 1773, has no application here. Dkt. No. 210-4 at 8-9. As the Court has previously observed, "[r]equiring each named plaintiff to establish specific personal jurisdiction over defendants in this Court is the proper approach under *BMS* and its precedents." *Sharpe v. Puritan's Pride, Inc.*, No. 16-cv-06717-JD, 2019 WL 188658, at *4 (N.D. Cal. Jan. 14, 2019).

For purposes of this analysis, the "proper focus...is on the defendant and its connection to the forum." *Id.* Plaintiffs argue that their "claims center on the operation of privacy-violative software in Subway Surfers, a product of the joint venture between Kiloo, Sybo, and the California SDKs. The very purpose of that joint venture is to extract users' Personal Data from their devices, including those in New York, and to send that data to the SDK Defendants -- all but one of whom are located in California -- where the data is analyzed and monetized for Sybo's benefit." Dkt. No. 210-4 at 10. Tellingly, plaintiffs make these arguments without any citations to their complaint. The complaint makes no such factual allegations about the existence of a joint venture.

In *Bristol-Myers Squibb*, 137 S.Ct. at 1778, the United States Supreme Court found specific jurisdiction to be lacking over BMS for the non-California residents' claims about BMS's drug, Plavix, where "BMS did not develop Plavix in California, did not create a marketing strategy for Plavix in California, and did not manufacture, label, package, or work on the regulatory approval of the product in California." It was not enough that BMS "does sell Plavix in California." *Id.* Further, "[t]he bare fact that BMS contracted with a California distributor [was] not enough to establish personal jurisdiction in the State." *Id.* at 1783.

These observations fit plaintiffs' allegations against Sybo as they currently stand. Sybo's motion to dismiss the New York GBL § 349 claim is granted. Plaintiffs may amend the claim.

V. DEFENDANT KOCHAVA'S MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION (DKT. NO. 195)

In the *Disney* case, defendant Kochava moves to dismiss for lack of personal jurisdiction, arguing that it is a Delaware corporation headquartered in Sandpoint, Idaho, with no significant ties to California. It asserts that the most efficient judicial resolution and alternative forum is in Idaho. Dkt. No. 195.

As with defendant Sybo, plaintiffs argue for specific jurisdiction at most. Dkt. No. 207-4. For this motion, plaintiffs bear "the burden of establishing that jurisdiction is proper," *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008), and they have failed to meet that burden. Plaintiffs focus on two things, neither of which are sufficient. First, plaintiffs focus on their allegations that Kochava was aware that the Disney gaming apps would be engaged on children's mobile devices in California. Dkt. No. 207-4 at 4-5. But these allegations are insufficient. *See Erickson*, 2015 WL 4089849, at *3 ("personal jurisdiction 'must arise out of contacts that the "defendant *himself*" creates with the forum State' and...'the plaintiff cannot be the only link between the defendant and the forum' "; *Walden* rejected idea that "a defendant's knowledge of a plaintiff's forum connections and the foreseeability of harm there are enough in themselves to satisfy the minimum contacts analysis") (quoting *Walden v. Fiore*, 571 U.S. 277 (2014)).

***13** Plaintiffs' focus on Kochava's contract with California-based Disney is also misplaced. For specific jurisdiction to exist, plaintiffs' claims must "arise[ ] out of or relate[ ] to the defendant's forum-related activities." *Schwarzenegger*, 374 F.3d at 802. Plaintiffs here are not parties to the contract between Kochava and Disney, and are not suing for any breaches of that contract.

The Court consequently grants Kochava's motion to dismiss for lack of personal jurisdiction. The Court cannot, however, rule out the possibility that plaintiffs may be able to cure these deficiencies in their personal jurisdiction allegations against Kochava, and so the plaintiffs will be given one last opportunity to try again.

CONCLUSION

Plaintiffs may file amended complaints in the *Kiloo* and *Disney* actions by **June 13, 2019**, to address: (1) the Massachusetts GL 93A claim against all defendants in the *Disney* case; (2) the claims against Flurry, Inc., Oath (Americas) Inc. and Oath Inc. in the *Kiloo* case; (3) the New York GBL § 349(a) claim against Sybo in the *Kiloo* case ; and (4) the claims against Kochava in the *Disney* case. The amended complaints may not add any new claims or defendants without leave of Court. Defendants' motions to dismiss are otherwise denied.

IT IS SO ORDERED.

Dated: May 22, 2019

JAMES DONATO

United States District Judge

All Citations

Slip Copy, 2019 WL 2211316

Footnotes

1 The Court refers to the cases by the lead developer defendant's name, as the parties do.

2 The thirty-four states are Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington and West Virginia.

3 The Court grants the pending requests to take judicial notice of these documents, Dkt. Nos. 196, 209, 212, 215, which are not germane to the Court's analysis in any event. Defendants' objection to plaintiffs' "demonstrative" used at the hearing on these motions, Dkt. No. 252, is overruled, though that demonstrative, too, did not impact the outcome here.

End of Document